El pasado 23 de abril, se llevó a cabo el diálogo sobre “Estrategias empresariales para la protección de datos y la agenda 2030 para el desarrollo sostenible", evento paralelo del III Foro de los Países de América Latina y el Caribe sobre el Desarrollo Sostenible, en la sede de la CEPAL.

Los temas discutidos se enmarcan en los **Objetivos de Desarrollo Sostenible** (ODS) 16 y 17 de una manera amplia. En ellos se hace referencia a la necesidad de crear a todo nivel, tanto público como privado, instituciones eficaces y transparentes que rindan cuentas sobre sus acciones y que sean capaces de atender aquellas prácticas reñidas con la ley como, por ejemplo, la corrupción, el soborno, etc. Por otra parte, el ODS 9 habla sobre el apoyo al desarrollo de tecnologías de información en los países en desarrollo, garantizando un entorno normativo propicio para, por ejemplo, la diversificación industrial, entre otras cosas.

Dos fueron las presentaciones principales con visiones complementarias desde el marco normativo y la empresa. La primera a cargo del Senador Felipe Harboe, quien presentó, el contexto nacional e internacional (el convenio de Budapest) en el que se circunscribe la propuesta de ley sobre protección de datos y ciberseguridad, actualmente en discusión en el Congreso chileno. Como premisa, un cambio de era basada en la gestión de los datos que incluye entre otras cosas la exportación de servicios globales, regulaciones adecuadas con incentivos a la industria y protección a los consumidores.

Resaltó la importancia de la economía digital para el desarrollo de Chile y la identificación de aquellos elementos o estándares clave, de un marco normativo amplio que identifica derechos, principios y un estándar propio que cubran las principales áreas consideradas en otros marcos de referencia para Chile como el modelo europeo (GDPR) y el modelo APEC.

Se hizo hincapié en el **consentimiento válido e inequívoco como fuente de licitud** del tratamiento de la información que asegura amplitud, protección y seguridad**.** No existe una cultura de protección de datos. Ellos pertenecen a las personas que los generan, no a las empresas que los usan. En América Latina no hay conciencia sobre el valor de los datos. La transferencia internacional de datos tiene que estar garantizada por normas con estándares iguales o superiores a las leyes nacionales y avalados por modelos de prevención de infracciones debidamente registrados y certificados.

Se calcula que los costos asociados a los ciber crímenes para las empresas alcanzan alrededor de US$2 trillones. El aumento de las inversiones en ciberseguridad ronda el 7%. En 2019, se calcula la venta de tecnologías en ciberseguridad en alrededor de los US$ 90 mil millones. Se espera que América Latina invierta en ciberseguridad alrededor de US$ 214 mil millones de dólares. Para contrarrestar los efectos de los ataques cibernéticos, que afectan fundamentalmente la reputación de las empresas - su principal activo -. Se requiere de un esfuerzo multilateral de largo plazo como la homologación de estándares y contar con legislaciones adecuadas, instituciones sólidas, responsables y con un entrenamiento adecuado que refuerce las capacidades técnicas y logísticas. Además, contar con un gobierno corporativo que incorpore el tema en la estructura de gobernanza de la empresa, en la estrategia del negocio, y que comprenda la magnitud de los riesgos que involucra.

Desde la perspectiva empresarial, Yoab Bitrán advirtió la falta de correlación entre la conciencia de la importancia de la ciberseguridad y la estrategia empresarial. La preocupación de las empresas sobre los riesgos asociados a los temas de protección de datos y la ciberseguridad contrasta con la baja presencia en las prioridades, en los presupuestos, y en el tiempo que se le dedica al tema desde el gobierno corporativo. Más que la falta de protocolos y estándares, **la complejidad estriba en la gestión de la seguridad cibernética y en asignarle un lugar prioritario**.

Sugirió **seis medidas** para avanzar en la implementación de las políticas de ciberseguridad al interior de la empresa: i) deben ser simples apoyadas por protocolos más técnicos, deben ser accesibles y evolutivas con una tendencia hacia la simplificación; ii) la construcción de una cultura al interior de la empresa, desde del directorio alineado con la relevancia del tema (*tone at the top*) y que permee al resto de la empresa en el mismo sentido, utilizando un lenguaje accesible para el conjunto de los empleados; iii) al frente del tema debe estar un alto ejecutivo, encargado de diseminar la cultura de la ciberseguridad a todos los niveles de la organización, no solo a los técnicos (CISO, TI); iv) debe contar con programas de capacitación: efectivos, relevantes, dirigidos y aplicados desde una óptica de *compliance,* creando conciencia en los empleados sobre ser la primera línea de defensa; v) sobre la debida diligencia se deben verificar los estándares de ciberseguridad de los socios, proveedores y terceras partes en general; e vi) integrar la política de ciberseguridad y protección de datos a las operaciones del negocio, sugiere la incorporación de temas de *compliance* a la evaluación de desempeño de los empleados.

En relación a América Latina, existe una brecha normativa con los países desarrollados que se debe ir cerrando a través de un trabajo multilateral y en alianzas público – privadas. Sugiere que empresas que operan en países con **normativas débiles o inexistentes, colaboren con *stakeholders* y reguladores para avanzar hacia la implementación de estándares**, lo que permite nivelar la cancha y competir en mejores condiciones.

En cuanto a las empresas multinacionales con presencia en varias jurisdicciones de América Latina deben adaptar como estándar global la regulación más estricta entre los países donde operan. Ello las mantiene en mejor posición frente a futuros cambios normativos a nivel local y regional.

En los **comentarios** de las empresas se hizo hincapié en la falta de una cultura de ciberseguridad en la región en general. Para la estrategia de digitalización de procesos se requiere necesariamente la ciberseguridad. Una estrategia trasversal que considere a los clientes, proveedores y empleados. Se requiere de políticas globales y parciales que permitan permear a toda la compañía y atienda todos los temas y áreas asociados al éxito de la estrategia del negocio, como el control interno. Es importante un marco normativo básico, pero también un trabajo de prevención y técnico.

Las plataformas de internet mutan de manera de irse adaptando a los nuevos estándares internacionales como los GDPR de la UE, lo que lleva a cambios culturales, económicos y también

a una nueva institucionalidad. Ejemplos de ello son el comercio electrónico, las metodologías de análisis de riesgo, la localización de los datos y las nubes, entre otras.

Existen disparidades en el tratamiento de los datos a nivel nacional y regional en una misma jurisdicción por parte de una empresa, lo cual también está asociado a una falta de cultura organizacional en materia de protección de datos y de ciberseguridad y una realidad económica regional con impacto en la población de dichas localidades.

Finalmente, en materia normativa, existe la idea generalizada que **la ley es tardía en relación a la evolución acelerada de la tecnología**, ello requiere de un esfuerzo por adaptar los marcos jurídicos a las necesidades del proceso digital. Existe la propuesta de generar **leyes – marco** de fácil adaptación y que permitan adelantarse a los desarrollos tecnológicos de manera expedita.